REMARKS

Claims 1-33 are presented for examination, with Claims 1, 10, 20, 25, and 30-33 being in independent form. Favorable reconsideration is requested.

Claims 1-3, 6-8, 10-14, 16, 17, 20, 21, 25, and 27 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 5,341,425 to Wasilewski et al. Claims 4, 5, 9, 15, 18, 19, 22-24, and 28-33 were rejected under 35 U.S.C. § 103(a) as being obvious from Wasilewski in view of U.S. Patent 5,319,705 to Halter et al.

Claim 1 is directed to a data processing apparatus including reception means, first encryption means, generating means, multiplexing means, and transmitting means. The reception means receives a plurality of transmitting requests of object data, and the first encryption means encrypts at least a predetermined portion of the object data using first key data to produce encrypted object data. The generating means generates seed information which allows the first key data to be obtained therefrom, the seed information being generated after the reception means receives the transmitting requests. The multiplexing means multiplexes the plurality of object data and the encrypted object data to generate a data stream. The transmitting means individually transmits the seed information and the data stream, the seed information being transmitted after the reception means receives the transmitting requests.

Among other notable features of Claim 1, are that the transmitting requests are received, then encrypted object data and seed information are individually transmitted. The seed information is generated after the transmitting requests are received, and allows first key data used to produce the encrypted object data to be obtained therefrom.

The features of Claim 1 can make it easier to assure security than by transmitting the actual key itself used for encryption, or transmitting a key and seed information together with encrypted data. Also, by virtue of the features of Claim 1, security can be maintained at a reproducing side without the necessity to safely keep the seed information, since the seed information is generated to be transmitted after receiving the transmitting requests.

Wasilewski et al., as understood by Applicants, relates to encrypting data at a plurality of data transmission sites for transmission to a reception site. A set of data is encrypted at each of a plurality N of transmission sites for transmission to and subsequent decryption at at least one reception site. Each of the N transmission sites is provided with a broadcast key unique to that transmission site and a system key that is the same for all transmission sites. At each transmission site, the system key and the broadcast key unique to that transmission site are convolved in a predetermined manner to generate a unique data encryption key for that transmission site. At each transmission site, a set of data is then encrypted with the unique data encryption key generated at that site. The sets of data uniquely encrypted at each transmission site are then transmitted to the reception site. There is stored, in a memory at the reception site, the system key and each of the broadcast keys to enable a selected one of the encrypted sets of data to be decrypted at the reception site.

The Examiner's comments set forth in the Advisory Action (specifically those on the Continuation Sheet) have been thoroughly reviewed, and it is respectfully submitted that the Examiner has not addressed the arguments presented in the Response After Final Action filed on December 5, 2005. Applicants therefore repeat all of the

arguments presented in the Response After Final Action in their entirety, and further offer the following remarks which specifically address the Examiner's comments set forth in the Advisory Action.

In the Response After Final Action, Applicants noted that nothing has been found in Wasilewski that would teach or suggest that (1) transmitting requests are received and then encrypted object data and seed information, which allows first key data used to produce the encrypted object data to be obtained therefrom, are individually transmitted, and (2) the seed information is generated to be transmitted *after* receiving the transmitting requests, as recited in Claim 1.

In the Advisory Action the Examiner states:

> The request for reconsideration has been considered but does NOT place the application in condition for allowance because: As understood the encryption information and the seed are received after a request, all cryptographic systems inherently receive a request before transmitting encrypted information. As to the individual transmissions that would depend upon the architecture and protocols required for the communication.

It is respectfully submitted that the Examiner's comments do not respond in any way to the arguments presented in the Response After Final Action. The Examiner states generally that "all cryptographic systems" inherently receive a request before transmitting encrypted information, but the terms of Claim 1 require that (1) transmitting requests are received and then encrypted object data and seed information, which allows first key data used to produce the encrypted object data to be obtained therefrom, are individually transmitted, and (2) seed information is *generated* to be transmitted *after* receiving the transmitting requests. As was noted in the Response After Final Action, the system and broadcast keys of Wasilewski et al. are provided *initially* on both the

transmission and reception sides (see, e.g., column 3 of that patent), and there is no teaching or suggestion in that patent that they are provided *after* transmitting requests are received. The Examiner has not addressed this point. There is also no teaching or suggestion in Wasilewski et al. that its program key is generated after transmitting requests are received (see, e.g., column 9, lines 30-35 of that patent). The Examiner has not addressed this point either. Applicants agree that ordinarily information is not transmitted until it is requested, but that is not relevant to the arguments Applicants are making.

The Examiner further states in the Advisory Action: "As to the individual transmissions that would depend upon the architecture and protocols required for the communication." However, this statement is merely a general observation, and does not provide a teaching of the terms of Claim 1.

It is respectfully submitted that the Examiner has not responded in any meaningful way to the arguments presented in the Response After Final Action distinguishing the claims over Wasilewski et al. In particular, nothing has been found in Wasilewski that would teach or suggest that (1) transmitting requests are received and then encrypted object data and seed information, which allows first key data used to produce the encrypted object data to be obtained therefrom, are individually transmitted, and (2) the seed information is generated to be transmitted *after* receiving the transmitting requests, as recited in Claim 1.

Accordingly, Claim 1 is believed to be clearly allowable over Wasilewski et al.

Independent Claims 10, 20, and 25 recite features similar in respect of the foregoing arguments to those of Claim 1 discussed above, and therefore are also believed to be patentable over Wasilewski et al. for at least the reasons discussed above.

Independent Claims 30-33 also recite features similar in many relevant respects to those discussed above with respect to Claim 1. Moreover, nothing has been found in Halter et al. that would remedy the deficiencies of Wasilewski et al., discussed above in connection with Claim 1. Accordingly, Claims 30-33 are believed to be patentable over Wasilewski et al. and Halter et al., whether considered either separately or in any permissible combination (if any).

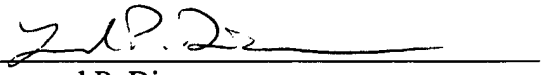
A review of the other art of record has failed to reveal anything which, in Applicants' opinion, would remedy the deficiencies of the art discussed above, as references against the independent claims herein. Those claims are therefore believed patentable over the art of record.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,



Leonard P. Diana
Attorney for Applicants
Registration No.: 29,296

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200